II. SPECIFICATION AMENDMENTS

The paragraph on page 2, lines 5-11,

A « pseudo-random permutation » is a permutation generated by a computer program that is fairly simple to compute from a secret key K having the following property: a person who does not know~~known~~ the key K is in practice incapable of distinguishing a permutation of this kind from a truly random permutation (with the same input and output sizes), because the number of computations needed in order to distinguish them by known methods far exceeds what is possible in realistic terms.

The paragraph on page 3, lines 14-27,

In the prior art, there are other known enciphering solutions not based on permutations, i.e. not based on bijection. However, inasmuch as it is sought to~~ce~~ carry out a reversible encryption, it must be ensured that the result of an enciphering is unique. Thus, at present, in certain applications, in order to ensure the uniqueness of the enciphering, certain industrialists or operators have, for many years, being been storing all the digit strings generated. They may thus ensure that each string is new because, if they generate an already used string, they detect it and do not put this string into circulation again but generate another string. However, such a method is costly and proves in the long run to be inconvenient because it soon calls for a great deal of available memory space and large and quickly accessible backup means located in highly secured premises. Furthermore, the number of computations to be made increases with the number of values already generated, and therefore increases with time.